CA Network Flow Analysis

Manuel d'installation

9.1.1

La présente documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si (i) un autre accord régissant l'utilisation du logiciel CA mentionné dans la Documentation passé entre vous et CA stipule le contraire ; ou (ii) si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2012 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 1 : Introduction 7

Chapitre 2 : Configuration requise pour Microsoft Windows Server 9

Configuration requise pour les systèmes d'exploitation Windows : 10
Navigateurs Web pris en charge (Windows) 11
Configuration matérielle requise pour une configuration distribuée (Windows) 12
Configuration matérielle requise pour un système autonome 13
Configuration du pare-feu 14
Installation des applications Adobe 15
Activation d'IIS, de COM+ et d'ASP (Windows) 15
Installation du service SNMP et du serveur SMTP (Windows) 18
Configuration de l'expiration du contenu Web (Windows) 19
Configuration de public en tant que nom de communauté accepté (Windows) 20
Configuration du format d'adresse IP sur les serveurs Windows 21
Configuration de restrictions de relais SMTP (Windows) 22
Activation de la prévention d'exécution des données (Windows) 23
Configuration de la corbeille (Windows) 24
Désactivation des services non requis (Windows) 25
Prévention des faux positifs au niveau des événements (Windows) 26

Chapitre 3 : Configuration requise pour les serveurs Linux 27

Configuration système requise pour les serveurs Linux 27
Configuration de SNMP sur les serveurs Linux 28
Désactivation du pare-feu iptables pour les serveurs Linux 30
Désactivation de la mise en réseau IPv6 sur les serveurs Linux 31

Chapitre 4 : Installation du logiciel 33

Conditions préalables 33
Installation des composants sur un serveur Windows autonome 35
Installation du composant de collecte sur un serveur Windows 37
Installation du composant de collecte sur un serveur Linux 39
Installation de la console sur un serveur Windows 41

Chapitre 5 : Tâches de post-installation 43

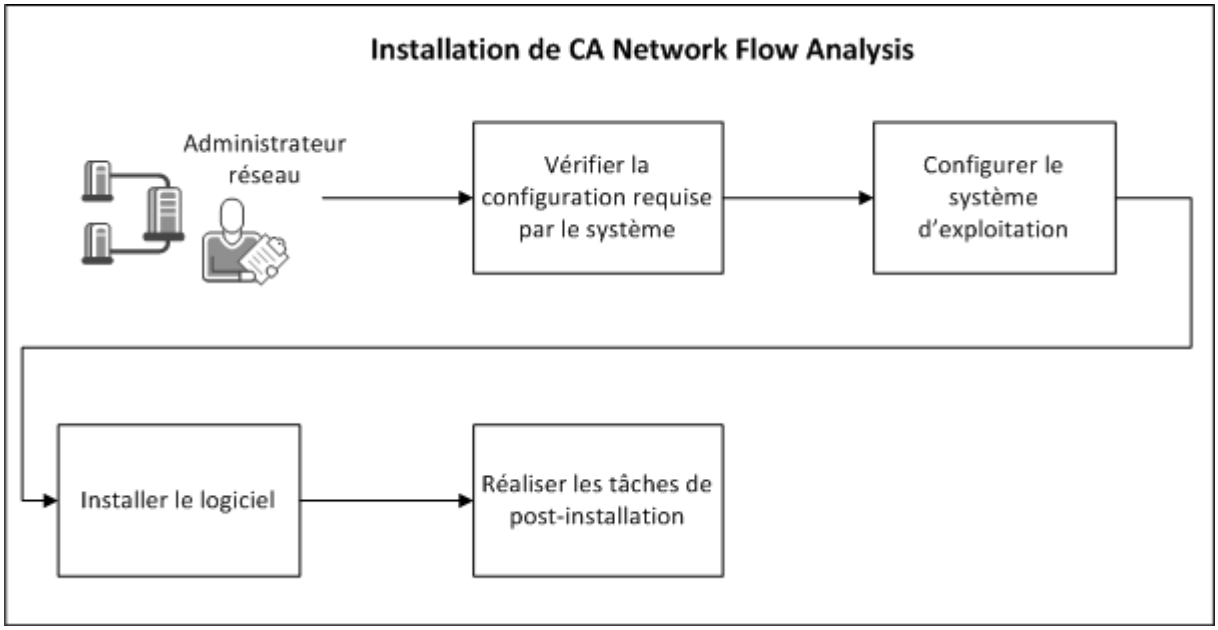
Procuration et installation de licences de produit (Windows) 43
Synchronisation de l'heure système (Windows) 44
Mise à jour de la liste des sites Internet approuvés (Windows) 44
Modification des listes de contrôle d'accès au routeur (Windows) 45

Index 47

Chapitre 1 : Introduction

CA Network Flow Analysis vous aide à déterminer de quelle manière le trafic des applications affecte vos performances réseau.

Le diagramme suivant décrit le processus d'installation de CA Network Flow Analysis.


Installation de CA Network Flow Analysis
Administrateur réseau
Vérifier la configuration requise par le système
Configurer le système d'exploitation
Installer le logiciel
Réaliser les tâches de post-installation

Chapitre 2 : Configuration requise pour Microsoft Windows Server

Lorsque vous vous procurez du matériel auprès de CA Technologies, tous les composants sont livrés avec le système d'exploitation et les paramètres de sécurité déjà configurés. Utilisez les rubriques de cette section pour vérifier les paramètres ou pour les mettre à jour suivant les besoins de votre organisation.

Lorsque vous achetez le logiciel uniquement, configurez et sécurisez le système d'exploitation comme décrit dans cette section.

Un administrateur de serveur doit procéder à l'installation de CA Network Flow Analysis.

Avant de commencer, copiez tous les fichiers dont vous avez besoin sur le serveur d'installation. Après avoir sécurisé le système d'exploitation, vous pouvez ne pas avoir accès aux dossiers partagés qui contiennent les fichiers.

Ce chapitre traite des sujets suivants :

Configuration requise pour les systèmes d'exploitation Windows : (page 10)
Navigateurs Web pris en charge (Windows) (page 11)
Configuration matérielle requise pour une configuration distribuée (Windows) (page 12)
Configuration matérielle requise pour un système autonome (page 13)
Configuration du pare-feu (page 14)
Installation des applications Adobe (page 15)
Activation d'IIS, de COM+ et d'ASP (Windows) (page 15)
Installation du service SNMP et du serveur SMTP (Windows) (page 18)
Configuration de l'expiration du contenu Web (Windows) (page 19)
Configuration de public en tant que nom de communauté accepté (Windows) (page 20)
Configuration du format d'adresse IP sur les serveurs Windows (page 21)
Configuration de restrictions de relais SMTP (Windows) (page 22)
Activation de la prévention d'exécution des données (Windows) (page 23)
Configuration de la corbeille (Windows) (page 24)
Désactivation des services non requis (Windows) (page 25)
Prévention des faux positifs au niveau des événements (Windows) (page 26)

Configuration requise pour les systèmes d'exploitation Windows :

Les serveurs Microsoft Windows qui hébergent des composants CA Network Flow Analysis doivent répondre à la configuration requise suivante.

Microsoft Windows 2008 R2, Standard Edition ou Enterprise Edition sur un processeur 64 bits

- Le dernier Service Pack et toutes les mises à jour critiques installées
- .NET Framework 3.5 SP1
- JRE (environnement d'exécution Java) 1.6 ou ultérieure
- Langue anglaise ou l'un des packs linguistiques suivants :
  - Chinois (simplifié)
  - Français (France)
  - Japonais
- Résolution d'affichage de 1024x768 (XGA) minimum
- *Console NFA et serveurs autonomes :* ASP.NET 2.0 installé, y compris l'accès au réseau COM+, IIS et ASP. ASP.NET 2.0 comprend .NET Framework 3.5 SP1.
- Le système d'exploitation configuré tel que décrit dans ce document, y compris l'activation du protocole SNMP.
- (Recommandé) Option Connexion Bureau à distance activée pour permettre à l'administrateur d'accéder à distance.

Remarques :

- CA Network Flow Analysis 9.1.1 prend en charge l'installation sur des serveurs avec des adresses IPv4. L'installation des serveurs avec des adresses IPv6 n'est pas encore prise en charge.
- Il est recommandé de configurer un contrôleur d'interface réseau unique sur chaque serveur.
- La configuration requise décrite dans cette section s'applique aux déploiements physiques et virtuels.

Navigateurs Web pris en charge (Windows)

L'accès à la console NFA est pris en charge pour les navigateurs suivants :

- Microsoft Internet Explorer version 7 ou ultérieure (version 8 recommandée)

  Remarque : Pour configurer CA Network Flow Analysis et utiliser ses données dans la console CA Performance Center, utilisez Internet Explorer 8 avec le mode de compatibilité désactivé. Pour travailler directement dans CA Network Flow Analysis, vous pouvez utiliser Internet Explorer 7 ou 8 avec le mode de compatibilité activé ou désactivé.

  Si les outils de développement d'Internet Explorer 8 sont installés, vous pouvez désactiver le mode de compatibilité pour la session actuelle du navigateur :

  a. Appuyez sur la touche F12.

  b. Cliquez sur l'élément Mode navigateur dans le menu principal.

  c. Sélectionnez Internet Explorer 8.

  Si une politique de votre entreprise vous oblige à utiliser Internet Explorer 8 en mode de compatibilité, vous pouvez utiliser Internet Explorer 7 ou Firefox.

- Mozilla Firefox versions 8.x - 10.x

  Remarque : CA Performance Center a été testé avec Mozilla Firefox 8.0.

  D'autres navigateurs ou versions de navigateur peuvent fonctionner avec CA Network Flow Analysis, mais ils n'ont pas été testés.

Configuration matérielle requise pour une configuration distribuée (Windows)

Dans une configuration *distribuée*, la console NFA et le composant de collecte sont installés sur des serveurs distincts.

La solution CA Network Flow Analysis a été testée avec la configuration matérielle recommandée suivante. La configuration requise peut varier selon le nombre d'interfaces, d'applications et d'utilisateurs présents sur votre réseau.

Remarque : Les spécifications recommandées ci-dessous s'appliquent aux déploiements physiques et virtuels. La section Configuration requise indique la configuration des appliances CA qui sont actuellement fournies. Vous pouvez exécuter CA Network Flow Analysis avec des configurations qui ne répondent pas à ces spécifications, mais les performances s'en verront affectées. Vous pouvez également exécuter CA Network Flow Analysis avec une configuration supérieure.

Serveur de la console NFA

Le serveur qui héberge la console NFA doit répondre aux spécifications minimum recommandées suivantes.

- Processeur quadruple coeur de 2,26 GHz
- 3 Go de mémoire RAM
- Trois disques durs SAS de 146 Go et 10 000 tr/min en configuration RAID 5
- Port LAN de 1 Go
- Partition pour le lecteur C avec 12 Go d'espace disponible pour le système d'exploitation
- Partition pour le lecteur D ou un autre lecteur distinct avec 41 Go pour les fichiers d'installation de CA Network Flow Analysis et 300 Go minimum d'espace disponible pour les données

Serveur du composant de collecte

Le serveur qui héberge le composant de collecte doit répondre aux spécifications minimum recommandées suivantes.

- Deux processeurs quadruple coeur de 2,26 GHz
- 12 Go de RAM
- Six disques durs SAS de 300 Go et 10 000 tr/min en configuration RAID 5
- Port Ethernet de 1 Go
- Partition pour le lecteur C avec 12 Go d'espace disponible pour le système d'exploitation
- Partition pour le lecteur D ou un autre lecteur distinct avec 41 Go pour les fichiers d'installation de CA Network Flow Analysis et 1,5 To minimum d'espace disponible pour les données

Configuration matérielle requise pour un système autonome

Une configuration *autonome* est un serveur unique sur lequel la console NFA et le composant de collecte sont installés.

La solution CA Network Flow Analysis a été testée avec la configuration matérielle recommandée suivante. La configuration requise peut varier selon le nombre d'interfaces, d'applications et d'utilisateurs présents sur votre réseau.

Remarque : Les spécifications recommandées ci-dessous s'appliquent aux déploiements physiques et virtuels. La configuration requise représente la configuration optimale appliquée aux appliances CA qui sont actuellement fournies. Vous pouvez exécuter CA Network Flow Analysis sur des configurations qui ne répondent pas à ces spécifications, mais les performances s'en verront affectées.

La configuration requise minimum du serveur est la suivante :

- Processeur quadruple coeur de 2,26 GHz
- 3 Go de mémoire RAM
- Trois disques durs SAS de 146 Go et 10 000 tr/min en configuration RAID 5
- Port LAN de 1 Go
- Partition pour le lecteur C avec 12 Go d'espace disponible pour le système d'exploitation
- Partition pour le lecteur D ou un autre lecteur distinct avec 41 Go pour les fichiers d'installation de CA Network Flow Analysis et 300 Go minimum d'espace disponible pour les données

Configuration du pare-feu

Pour que CA Network Flow Analysis fonctionne correctement dans un environnement protégé par un pare-feu, les ports de communication suivants doivent être ouverts. La liste suivante récapitule les ports du pare-feu qui doivent être ouverts pour permettre aux composants CA Network Flow Analysis de communiquer.

En sortie à partir de la console NFA

- TCP 25 [rapports par courriel SMTP]
- UDP 53

Console NFA vers les composants de collecte

- TCP 80 [services Web SNMP]
- TCP 3307 [CA MySQL]
- TCP 3308 [MySQL]
- TCP 8066 [appels services Web SOAP]
- TCP 8080 [examen des flux]
- UDP 161 [service de surveillance]

Composant de collecte vers les routeurs (interface SNMP, en lecture seule)

- UDP 161 [interrogation SNMP]

Composant de collecte vers la destination d'interruption

- UDP 162 [interruptions]

Routeurs vers les composants de collecte

- UDP 9995 [flux]

Administrateurs et utilisateurs vers la console NFA

- TCP 80 [accès IUG et services Web SNMP]
- TCP 8381 [authentification unique]
- TCP 8681 [génération de rapports de la RIB (base d'informations de génération de rapports)]

Administrateurs vers chaque serveur

- TCP 3389 [bureau à distance]
- TCP 5800, 5801, 5900, 5901 [VNC]

(obligatoire si le bureau à distance et VNC sont utilisés).

Installation des applications Adobe

Adobe Flash Player est requis pour afficher les rapports et les statuts. Installez la dernière version de Flash Player à partir de http://get.adobe.com/flashplayer/.

Adobe Acrobat Reader est requis sur les systèmes utilisés pour afficher la documentation du produit au format PDF. Installez la dernière version d'Acrobat Reader à partir de http://get.adobe.com/reader/.

Activation d'IIS, de COM+ et d'ASP (Windows)

Activez IIS, IIS 6 Management Compatibility, l'accès réseau COM+ et ASP sur un serveur d'installation autonome ou un serveur d'installation de la console NFA.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'administrateur.
2. Sélectionnez Démarrer, Outils d'administration, Gestionnaire de serveur.

   La fenêtre Gestionnaire de serveur s'ouvre.
3. Développez la liste Rôles dans l'arborescence Console à gauche.

4. Ajoutez le service de rôle IIS :
    a. Cliquez sur le lien Serveur d'applications dans la liste Rôles de l'arborescence Console à gauche.

       La vue Serveur d'applications s'ouvre dans le volet droit.

    b. Dans la section Services de rôle, cliquez sur Ajouter des services de rôle.

       L'Assistant Ajouter des services de rôle s'ouvre à la page Sélectionner les services de rôle.

    c. Cochez la case Prise en charge du serveur Web (IIS).

       Un message de confirmation apparaît.

    d. Dans le message de confirmation, cliquez sur Ajouter les services de rôle requis.

       L'option Prise en charge du serveur Web (IIS) est mise en surbrillance dans la page Sélectionner les services de rôle.

5. Ajoutez le service de rôle COM+ :
    a. Cochez la case Accès réseau COM+.

       Un message de confirmation apparaît.

    b. Dans le message de confirmation, cliquez sur Ajouter les services de rôle requis, puis sur Suivant.

       La page Serveur Web (IIS) de l'Assistant Ajouter des services de rôle s'ouvre.

6. Activez IIS 6 Management Compatibility :
    a. Cliquez à nouveau sur Suivant.

       Une liste de services de rôle s'affiche dans l'Assistant.

    b. Cochez la case IIS 6 Management Compatibility dans la section Outils de gestion de la liste, puis cliquez sur Suivant.

       La page Confirmer les sélections pour l’installation récapitule vos actions et affiche les messages associés.

7. Installez les options et les rôles de service IIS et COM+ que vous avez sélectionnés :
   a. Cliquez sur Installer.

      La page d'avancement s'affiche jusqu'à ce que l'installation se termine, puis la page Résultats s'ouvre.

   b. (Facultatif) Cliquez sur Imprimer, envoyer ou enregistrer le rapport d'installation, vérifiez les informations, puis fermez la page.

      La page Rapport d'installation affiche un récapitulatif de vos modifications, des informations sur les modifications et l'emplacement du journal d'installation complet.

   c. Cliquez sur Fermer.

      La page Résultats se ferme.

8. Ajoutez et installez le service de rôle ASP :
   a. Cliquez sur le lien Serveur Web (IIS) dans la liste Rôles de l'arborescence Console à gauche.

      La vue Serveur Web (IIS) s'ouvre dans le volet droit.

   b. Dans la section Services de rôle, cliquez sur Ajouter des services de rôle.

      L'Assistant Ajouter des services de rôle s'ouvre à la page Sélectionner les services de rôle.

   c. Dans la liste, cochez la case ASP sous Développement d'applications et cliquez sur Suivant.

      La page Confirmer les sélections pour l'installation récapitule vos actions et les messages associés.

   d. Cliquez sur Installer.

      La page d'avancement s'affiche jusqu'à ce que l'installation se termine, puis la page Résultats s'ouvre.

   e. (Facultatif) Cliquez sur Imprimer, envoyer ou enregistrer le rapport d'installation, vérifiez les informations, puis fermez la page.

      La page Rapport d'installation affiche un récapitulatif de vos modifications, des informations sur les modifications et l'emplacement du journal d'installation complet.

   f. Cliquez sur Fermer.

      La page Résultats de l'installation se ferme.

9. Quittez la fenêtre Gestionnaire de serveur.

Installation du service SNMP et du serveur SMTP (Windows)

Installez le service SNMP et le serveur SMTP sur un serveur d'installation autonome ou un serveur d'installation de console NFA.

Le protocole SNMP est requis par les services de surveillance. Le service SMTP est un composant IIS utilisé pour l'envoi des courriels sortants.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'administrateur.
2. Accédez au menu Outils d'administration, Gestionnaire de serveur.

   La fenêtre Gestionnaire de serveur s'ouvre.
3. Cliquez sur Fonctionnalités dans l'arborescence Console à gauche.

   La fenêtre Gestionnaire de serveur affiche une liste des fonctionnalités installées sur le serveur.
4. Sous Résumé des fonctionnalités, cliquez sur Ajouter des fonctionnalités.

   La page Sélectionner des fonctionnalités affiche une liste des fonctionnalités installées disponibles dans l'Assistant Ajouter des fonctionnalités.
5. Dans la liste Fonctionnalités, sélectionnez Service SNMP.

   Un message de confirmation apparaît.
6. Cliquez sur Ajouter les fonctionnalités requises.

   La page de services Confirmer l'installation identifie les fonctionnalités à installer et affiche des messages importants sur l'installation.
7. Cliquez sur Installer.

   La page Progression de l'installation affiche l'avancement de l'installation. Lorsque l'installation est terminée, la page Résultats de l'installation identifie les nouvelles fonctionnalités et indique si vous devez redémarrer le serveur.
8. Cliquez sur Fermer.

   Un message vous demande si vous voulez redémarrer le serveur.

9. Cliquez sur Non.
10. Répétez les étapes 5 à 8 pour le serveur SMTP.

    Un message vous demande si vous voulez redémarrer le serveur.
11. Cliquez sur Oui.

    Après le redémarrage du serveur, la vue Fonctionnalités de la fenêtre Gestionnaire de serveur contient les dernières fonctionnalités installées.

Configuration de l'expiration du contenu Web (Windows)

Configurez IIS de façon à vous assurer que les données affichées sont actualisées. Lorsque le paramètre d'expiration immédiate du contenu Web est activé, le navigateur affiche une page mise à jour à partir du serveur plutôt qu'à partir du cache.

Remarque : Effectuez cette tâche pour un serveur d'installation autonome ou un serveur d'installation de console NFA.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'administrateur.
2. Accédez au menu Outils d'administration et double-cliquez sur Gestionnaire des services Internet (IIS).

   La fenêtre Gestionnaire des services Internet (IIS) s'ouvre.
3. Cliquez sur le nom du serveur dans le volet Connexions.

   Les fonctionnalités du serveur s'affichent dans le volet droit.
4. Double-cliquez sur l'icône En-têtes de réponse HTTP dans le groupe Fonctionnalités HTTP.

   La fenêtre affiche les en-têtes de réponse HTTP actuels.
5. Dans le volet Actions, cliquez sur Définir les en-têtes communs.

   La boîte de dialogue Définir les en-têtes communs s'ouvre.
6. Sélectionnez les options suivantes :
   - Case à cocher Expiration du contenu
   - Immédiatement

7. Cliquez sur OK.

   La boîte de dialogue Définir les en-têtes communs se ferme.

8. Fermez la fenêtre Gestionnaire des services Internet (IIS).

Configuration de public en tant que nom de communauté accepté (Windows)

Le nom de communauté public doit être accepté pour empêcher les erreurs d'interrogation et permettre aux composants CA Network Flow Analysis de fonctionner correctement.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'administrateur.
2. Accédez au menu Outils d'administration et double-cliquez sur Gestionnaire des services Internet (IIS).

   La fenêtre Gestionnaire des services Internet (IIS) s'ouvre.

3. Développez la liste Configuration dans l'arborescence Console à gauche.
4. Sous Configuration, cliquez sur Services.

   La liste Services s'ouvre.

5. Cliquez avec le bouton droit de la souris sur la ligne Service SNMP et sélectionnez Propriétés.

   La boîte de dialogue Propriétés du service s’ouvre.

6. Cliquez sur l'onglet Sécurité.
7. Cliquez sur Ajouter.

   La boîte de dialogue Configuration du service SNMP s’ouvre.

8. Spécifiez les options suivantes :
   - Droits de communauté : sélectionnez Lecture seule.
   - Nom de communauté : entrez **public**.
9. Cliquez sur Ajouter.

   La boîte de dialogue Propriétés du service affiche public dans la liste des noms de communauté acceptés.

10. Cliquez sur OK.

Configuration du format d'adresse IP sur les serveurs Windows

Vérifiez que les connexions pour vos serveurs d'installation Windows ne sont pas configurées pour utiliser des adresses IPv6.

Remarque : Les instructions suivantes ne sont effectives que si la configuration recommandée est respectée, c'est-à-dire qu'un contrôleur d'interface réseau unique est configuré pour chaque serveur.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'administrateur.
2. Ouvrez la fenêtre Connexions réseau :
   a. Pour cela, ouvrez le panneau de configuration et cliquez sur Réseau et Internet.

      La fenêtre Réseau et Internet s'ouvre.

   b. Cliquez sur Centre Réseau et partage.

      La fenêtre Centre Réseau et partage s'ouvre.

   c. Dans la partie gauche de la fenêtre, cliquez sur Modifier les paramètres de la carte.

      La fenêtre Connexions réseau s'ouvre.
3. Cliquez avec le bouton droit de la souris sur la connexion et sélectionnez Propriétés dans le menu.

   La boîte de dialogue Propriétés s'affiche.
4. Si la case Internet Protocol Version 6 (TCP/IPv6) est cochée, décochez-la.
5. Cliquez sur OK.

   Vos modifications sont enregistrées. La boîte de dialogue Propriétés se ferme.
6. Fermez la fenêtre Connexions réseau.

Configuration de restrictions de relais SMTP (Windows)

Vous pouvez contrôler les relais de messagerie vers le serveur virtuel IIS SMTP pour renforcer la sécurité. Lorsque le serveur virtuel SMTP est ouvertement accessible, un utilisateur peut facilement distribuer des spams.

Configurez des restrictions de relais de serveur virtuel SMTP pour permettre l'accès uniquement à l'ordinateur 127.0.0.1 et rejeter tous les autres. Les restrictions permettent uniquement aux ordinateurs sélectionnés de diffuser des messages via le serveur virtuel SMTP. Les autres ordinateurs ne peuvent pas diffuser de messages via ce serveur, même s'ils répondent aux exigences définies dans la boîte de dialogue Authentification.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'administrateur.
2. Installez la fonctionnalité de serveur SMTP (page 18).
3. Accédez au menu Outils d'administration et double-cliquez sur Gestionnaire des services Internet (IIS).

   La fenêtre Gestionnaire des services Internet (IIS) s'ouvre.
4. Développez votre serveur dans l'arborescence Console à gauche.

   Les détails du serveur sont affichés. Le serveur virtuel SMTP s'affiche sous votre serveur.

   Remarque : Si le serveur virtuel SMTP ne s'affiche pas, ajoutez la fonctionnalité de serveur SMTP (page 18).
5. Cliquez avec le bouton droit de la souris sur Serveur virtuel SMTP par défaut, puis cliquez sur Propriétés.

   La boîte de dialogue Propriétés du serveur virtuel SMTP par défaut s'ouvre.
6. Cliquez sur l'onglet Accéder, puis sur Relais.

   La boîte de dialogue Restrictions de relais s'ouvre.
7. Cliquez sur Ajouter.

   La boîte de dialogue Ordinateur s'affiche.
8. Spécifiez les paramètres suivants :
   - Sélectionnez Ordinateur unique.
   - Adresse IP : entrez **127.0.0.1**.

9. Cliquez sur OK.

   La boîte de dialogue Restrictions de relais affiche 127.0.0.1 dans la liste Ordinateurs. L'ordinateur avec l'adresse IP 127.0.0.1 a le statut Autorisé dans la colonne Accès.

10. Spécifiez les options de restrictions de relais suivantes :

    - Uniquement la liste ci-dessous : sélectionnée. Cette option autorise uniquement les ordinateurs répertoriés dans la liste Ordinateurs à diffuser des messages via le serveur virtuel SMTP.
    - Autoriser tous les ordinateurs qui s'authentifient avec succès à relayer, indépendamment de la liste ci-dessus : non sélectionnée.

11. Cliquez sur OK.

    La boîte de dialogue Propriétés du serveur virtuel SMTP s'ouvre. Avec les options que vous avez sélectionnées, uniquement les ordinateurs répertoriés peuvent diffuser des messages via le serveur virtuel SMTP. Les autres ordinateurs ne peuvent pas diffuser de messages via ce serveur, même s'ils répondent aux exigences définies dans la boîte de dialogue Authentification.

12. Cliquez sur OK.

    La boîte de dialogue Propriétés du serveur virtuel SMTP se ferme.

13. Dans la fenêtre Gestionnaire des services Internet (IIS), sélectionnez Fichier, Quitter.

Activation de la prévention d'exécution des données (Windows)

La stratégie Prévention de l'exécution des données (PED) vous aide à empêcher l'exécution de code à partir des pages de données. Il est fortement recommandé de l'activer.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'administrateur.
2. Ouvrez le Panneau de configuration.

3. Cliquez sur le lien Système.

   La fenêtre Système s'ouvre.

4. Cliquez sur le lien Paramètres système avancés.

   La boîte de dialogue Propriétés du système s'ouvre.

5. Cliquez sur l'onglet Avancé.

6. Cliquez sur Paramètres.

   La boîte de dialogue Options de performances s'affiche.

7. Cliquez sur l'onglet Prévention de l'exécution des données.

8. Sélectionnez Activer la prévention d'exécution des données pour les programmes et les services Windows uniquement.

9. Pour fermer la boîte de dialogue Options de performances, cliquez sur OK.

10. Cliquez sur OK pour fermer la boîte de dialogue Propriétés système.

    La PED est implémentée.

Configuration de la corbeille (Windows)

Vous pouvez configurer la manière dont les fichiers sont supprimés dans la corbeille.

Procédez comme suit:

1. Cliquez avec le bouton droit de la souris sur la corbeille et sélectionnez Propriétés.

   La boîte de dialogue Propriétés de la corbeille s’ouvre.

2. Sélectionnez Disque local (C:).

3. Sélectionnez Ne pas déplacer les fichiers vers la Corbeille. Supprimer immédiatement les fichiers lorsqu'ils sont effacés.

4. Cliquez sur Appliquer.

5. Répétez les étapes 2 à 4 pour chaque lecteur supplémentaire que vous voulez configurer.

6. Cliquez sur OK.

Désactivation des services non requis (Windows)

Utilisez la fenêtre Services pour désactiver les services inutiles.

Procédez comme suit:

1. Accédez au menu Outils d'administration.
2. Double-cliquez sur Services.

   La fenêtre Services s'affiche.
3. Cliquez avec le bouton droit de la souris sur les services suivants et sélectionnez Manuel ou Désactivé.

   Ne sélectionnez pas Arrêter ou les services démarreront à nouveau lors du redémarrage du serveur.

- Service de la passerelle de la couche Application
- Client de suivi de lien distribué
- Publication des ressources de découverte de fonctions
- Découverte de la topologie de la couche de liaison
- NetLogon
- Service Enumérateur d'appareil mobile
- Gestionnaire de connexions d'accès distant
- Ouverture de session secondaire
- Application d'assistance de la Console d'administration spéciale
- Téléphonie
- Gestion des applications
- Distributed Transaction Coordinator
- Accès du périphérique d'interface utilisateur
- Service Initiateur iSCSI de Microsoft
- Service Liste des réseaux
- Spouleur d'impression
- Accès à distance au Registre
- Carte à puce
- Détection SSDP
- Cliché instantané de volume
- Propagation du certificat
- Client DNS
- Assistance IP
- Planificateur de classes multimédias
- Service Connaissance des emplacements réseau
- Gestionnaire de connexion automatique d'accès distant
- Fournisseur d'un jeu de stratégie résultant
- Stratégie de retrait de la carte à puce
- Service Panneau de saisie Tablet PC
- Audio Windows

- Générateur de points de terminaison du service Audio Windows
- Service de découverte automatique de Proxy Web pour les services HTTP Windows
- Windows CardSpace
- Carte de performance WMI
- Système de couleurs Windows

Prévention des faux positifs au niveau des événements (Windows)

Créez une clé vide pour empêcher le service SNMP de journaliser des faux positifs au niveau des événements.

Procédez comme suit :

1. Ouvrez une invite de commande.
2. Exécutez la commande suivante :

```
reg add
HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConf
iguration
```

Chapitre 3 : Configuration requise pour les serveurs Linux

Ce chapitre traite des sujets suivants :

Configuration système requise pour les serveurs Linux (page 27)
Configuration de SNMP sur les serveurs Linux (page 28)
Désactivation du pare-feu iptables pour les serveurs Linux (page 30)
Désactivation de la mise en réseau IPv6 sur les serveurs Linux (page 31)

Configuration système requise pour les serveurs Linux

Pour une configuration distribuée, CA Network Flow Analysis prend en charge l'installation du composant de collecte sur les serveurs Linux qui correspondent à la configuration requise suivante :

- Red Hat Enterprise Linux 5.5 ou 5.6 sur un processeur 64 bits
- Langue anglaise ou l'un des packs linguistiques suivants :
  - Chinois (simplifié)
  - Français (France)
  - Japonais
- Deux processeurs quadruple coeur de 2,26 GHz
- 12 Go de RAM
- Six disques durs SAS de 300 Go et 10 000 tr/min en configuration RAID 5
- Port Ethernet de 1 Go
- Mozilla Firefox versions 3.x - 10.x

Si vous ne disposez pas d'assez d'espace disponible au niveau du répertoire /tmp et que vous ne pouvez pas configurer ce répertoire, déplacez-le. Exportez la variable d'environnement IATEMPDIR, pour définir un nouvel emplacement pour le répertoire temporaire Install Anywhere et sélectionnez un répertoire avec l'espace suffisant.

Remarques :

- CA Network Flow Analysis 9.1.1 prend en charge l'installation sur des serveurs avec des adresses IPv4. L'installation des serveurs avec des adresses IPv6 n'est pas encore prise en charge.
- La configuration requise décrite dans cette section s'applique aux déploiements physiques et virtuels.

Important : CA Network Flow Analysis requiert une résolution DNS. Si le DNS n'est pas configuré, ajoutez manuellement des entrées système au fichier /etc/hosts sur votre serveur.

Configuration de SNMP sur les serveurs Linux

Pour configurer un serveur Linux pour un composant de collecte, effectuez les tâches suivantes :

- Installez Net-SNMP s'il n'est déjà pas installé.
- Configurez le fichier de configuration Net-SNMP.
- Configurez SNMP pour qu'il se lance automatiquement lors du démarrage.
- Lancez le service snmpd.

Procédez comme suit:

1. Vérifiez que Net-SNMP se trouve sur le serveur d'installation. Dans le cas contraire, installez-le. Net-SNMP est requis pour la prise en charge de la fonctionnalité de surveillance.
   a. Ouvrez le gestionnaire de packages Linux et recherchez les listes qui contiennent net-snmp.

      Si vous ne trouvez aucune liste contenant net-snmp, Net-SNMP n'est pas installé :

   b. Récupérez Net-SNMP et installez-le s'il ne l'est pas déjà. Par exemple, vous pouvez récupérer Net-SNMP à partir du gestionnaire de packages Linux.
2. Connectez-vous en tant que root et ouvrez une invite shell.

3. Recommandation : copiez le fichier de configuration Net-SNMP dans le répertoire Netflow, en écrasant le fichier snmpd.conf non configuré. Pour activer l'interrogation SNMP de l'outil de surveillance pour le composant de collecte, vous devez effectuer cette opération.

   Remarque : Si vous avez un fichier de configuration snmp personnalisé et non un fichier par défaut sous /etc/snmp/snmp.conf, vous pouvez ignorer cette étape et mettre à jour votre fichier de configuration existant à la place. Dans ce cas, consultez un administrateur pour mettre à jour les paramètres requis afin qu'ils correspondent aux paramètres de l'exemple de fichier de configuration. Par exemple, vérifiez que la valeur de rocommunity est définie comme dans l'exemple de fichier de configuration.

   a. Recommandation : sauvegardez le fichier de configuration dans /etc, par exemple en entrant la commande suivante :
   `cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak`

   b. Accédez au répertoire Netflow :
   `cd <répertoire_installation>/Netflow`

   où <répertoire_installation> est le répertoire utilisé pour l'installation du composant de collecte /opt/CA/NFA/ ou un emplacement personnalisé.

   c. Copiez le fichier snmpd.conf dans le répertoire /etc/snmp en écrasant le fichier existant :
   `cp -i snmpd.conf /etc/snmp`

   d. Confirmez le remplacement lorsque vous y êtes invité.

   e. Vérifiez que le fichier de configuration est en place :
   `ls -l /etc/snmp/snmpd.conf`

   f. Vérifiez que le fichier de configuration dispose des autorisations appropriées :
   `chmod 600 snmpd.conf`

4. Configurez SNMP pour qu'il se lance automatiquement à chaque démarrage en entrant la commande suivante :
   `chkconfig snmpd on`

5. Démarrez le service SNMP de l'une des manières suivantes :

   - Entrez la commande :
   `service snmpd start`
   - Accédez aux services dans l'interface utilisateur, sélectionnez snmpd, Démarrer, puis cliquez sur Enregistrer.

   Le service SNMP démarre avec le paramètre de chaîne de communauté approprié.

Désactivation du pare-feu iptables pour les serveurs Linux

Il est recommandé de désactiver le pare-feu iptables et d'arrêter le service iptables sur chaque serveur Linux sur lequel un composant de collecte est installé. Si vous désactivez les iptables, assurez-vous que tous les ports requis sont ouverts et que les performances ne sont pas affectées.

Remarque : Si votre entreprise requiert l'utilisation d'iptables, vérifiez que tous les ports de pare-feu appropriés sont ouverts dans la liste Configuration du pare-feu (page 14). En outre, vérifiez que vous disposez d'un accès hôte local à hôte local complet. Cette opération est requise, car CA Network Flow Analysis utilise un accès RMI (appel de méthodes distantes).

Effectuez les opérations suivantes pour désactiver tous les niveaux d'iptables et permettre aux composants CA Network Flow Analysis de communiquer.

Procédez comme suit:

1. Connectez-vous en tant que root ou avec un compte d'utilisateur sudo.
2. Exécutez les commandes suivantes dans une fenêtre d'invite de commande :

   ```
   service iptables stop

   chkconfig iptables off

   chkconfig —-list |grep iptables
   ```

3. Examinez la sortie de la dernière commande et vérifiez que tous les niveaux iptables sont désactivés, comme dans l'exemple suivant :

   ```
   iptables 0:off 1:off 2:off 3:off 4:off 5:off 6:off
   ```

Désactivation de la mise en réseau IPv6 sur les serveurs Linux

Désactivez la mise en réseau IPv6 sur chaque serveur Linux sur lequel un composant de collecte est installé.

Remarque : Effectuez cette tâche avant d'ajouter le composant de collecte dans la console NFA. Si le protocole IPv6-format est activé lorsque vous ajoutez un composant de collecte dans la console NFA, il se lie automatiquement à une adresse IPv6 et les données ne sont pas reçues par CA Network Flow Analysis.

Pour désactiver la mise en réseau IPv6, modifiez les fichiers suivants :

- Le fichier de configuration de pilote de noyau modprobe.conf, qui se trouve par défaut dans le répertoire /etc.
- Le fichier de configuration de pilote RHEL network, qui se trouve par défaut dans le répertoire /etc/sysconfig.

Procédez comme suit :

1. Vérifiez que vous êtes connecté avec les droits root.
2. Modifiez le fichier modprobe.conf :
   a. Ouvrez le fichier /etc/modprobe.conf dans un éditeur de texte.
   b. Ajoutez la ligne suivante :
   ```
   install ipv6 /bin/true
   ```
   c. Enregistrez et fermez le fichier.

   Le fichier modprobe.conf est configuré de façon à ce que lorsque le système essaye de charger le module de noyau IPv6, la commande true est exécutée à sa place. La commande true n'effectue aucune action.
3. Modifiez le fichier réseau :
   a. Ouvrez le fichier /etc/sysconfig/network dans un éditeur de texte.
   b. Mettez à jour les lignes suivantes ou ajoutez-les pour qu'elles correspondent aux chaînes de texte affichées :
   ```
   NETWORKING_IPV6=no
   IPV6INIT=no
   ```
   c. Enregistrez et fermez le fichier.
4. Redémarrez le serveur :
   ```
   reboot
   ```

5. Vérifiez que le protocole IPv6 est désactivé.
   a. Dans un terminal, entrez la commande suivante :
      `lsmod | grep ipv6`

      Si la commande ne renvoie aucune sortie, le module du noyau IPv6 ne s'exécute pas, car il a été supprimé.
   b. Entrez la commande suivante :
      `/sbin/ifconfig`

      Vérifiez que la sortie contient uniquement des adresses IPv4 et aucune adresse IPv6.

Chapitre 4 : Installation du logiciel

Ce chapitre traite des sujets suivants :

Conditions préalables (page 33)
Installation des composants sur un serveur Windows autonome (page 35)
Installation du composant de collecte sur un serveur Windows (page 37)
Installation du composant de collecte sur un serveur Linux (page 39)
Installation de la console sur un serveur Windows (page 41)

Conditions préalables

Avant d'installer le logiciel CA Network Flow Analysis, effectuez les tâches suivantes :

- Installez CA Performance Center 2.0 dans votre environnement.

  Les administrateurs doivent utiliser CA Performance Center pour créer des utilisateurs et des rôles, définir des autorisations et créer des domaines.

  CA Network Flow Analysis r9.1.1 n'est pas compatible avec les versions précédentes de CA Performance Center.

- Supprimez les versions précédentes de CA Network Flow Analysis installées sur les serveurs qui hébergeront CA Network Flow Analysis r9.1.1.

  CA Network Flow Analysis 9.1.1 prend uniquement en charge les nouvelles installations.

  Vous ne pouvez pas mettre à niveau une version précédente vers la version 9.1.1. Les mises à niveau seront prises en charge dans une prochaine version de CA Network Flow Analysis.

- Affectez une adresse IP statique au serveur.

  Remarque : Affectez l'adresse IP du serveur du composant de collecte pour mettre en correspondance la destination d'exportation de flux qui est affectée à chaque routeur.

- Installez un logiciel antivirus.

- Désactivez les types de logiciels tiers suivants sur tous les serveurs qui hébergeront les composants CA Network Flow Analysis :

  - Les anti-espiogiciels
  - Les outils de surveillance et de maintenance de serveur comme SMS, SUS ou MoM

- Excluez les répertoires suivants des analyses en temps réel : C:\Windows\Temp, *<chemin_installation_NFA>* et tous ses sous-répertoires.

  Les analyses en temps réel de ces répertoires peuvent endommager la base de données.

- N'implémentez pas la compression de l'espace disque sur le serveur d'installation.

  La compression d'espace disque peut endommager la base de données et détériorer les performances système.

- Redémarrez tous les serveurs afin de vous assurer que les patchs de système d'exploitation disponibles sont appliqués.

- Récupérez les fichiers d'installation de CA Network Flow Analysis à partir du site de support technique de CA, puis effectuez l'une des tâches suivantes :

  - Gravez les fichiers ISO sur un CD-ROM ou un DVD.
  - Utilisez une application d'image ISO pour extraire le contenu des fichiers ISO. La plupart des applications d'image ISO sont gratuites.

- Extrayiez les fichiers suivants sur les serveurs sur lesquels vous voulez installer le logiciel :

  - RAConsoleSetup9.x.x.exe (installation de la console NFA sur les serveurs Windows).
  - NFHarvesterSetup9.x.x.exe (installation des composants de collecte sur les serveurs Windows).
  - NFHarvesterSetup9.x.x.bin (installation des composants de collecte sur les serveurs Linux).

Installation des composants sur un serveur Windows autonome

Une *configuration autonome* consiste en un serveur unique qui héberge la console NFA et le composant de collecte. Effectuez les opérations de cette rubrique pour installer les composants de CA Network Flow Analysis sur un serveur ou un ordinateur virtuel Windows unique.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'administrateur.
2. Installation du composant de collecte :
   a. Double-cliquez sur le fichier NFHarvesterSetup9.x.x.exe.

      La fenêtre de sélection de langue s'ouvre.

   b. Sélectionnez une langue, puis cliquez sur OK.

      La fenêtre Contrat de licence s'affiche.

   c. Lisez et acceptez les termes du contrat, puis cliquez sur Suivant.

      Votre système est testé pour vérifier qu'il répond à certaines conditions préalables. Si tel est le cas, la fenêtre Sélectionner le dossier d'installation s'ouvre.

   d. (Facultatif) Lorsque vous y êtes invité, cliquez sur Sélectionner pour modifier l'emplacement d'installation ou entrez le chemin d'accès au nouvel emplacement.

      L'emplacement par défaut est C:\CA\NFA. Il est recommandé d'installer les composants CA Network Flow Analysis sur le lecteur que vous avez configuré pour CA Network Flow Analysis, qui ne contient aucun système. La console NFA sera installée dans le même répertoire que celui du composant de collecte.

   e. Cliquez sur Suivant.

      (Facultatif) Lorsque vous y êtes invité, cliquez sur Sélectionner pour modifier l'emplacement d'installation de MySQL ou entrez le chemin d'accès au nouvel emplacement.

   f. Cliquez sur Suivant.

   g. (Facultatif) Lorsque vous y êtes invité, cliquez sur Sélectionner pour modifier l'emplacement temporaire d'installation ou entrez le chemin d'accès au nouvel emplacement.

h. Cliquez sur Suivant.

   La fenêtre Récapitulatif de la pré-installation s'ouvre.

i. Cliquez sur Installer.

   Le processus d'installation démarre. Les messages indiquent l'avancement de l'installation. Lorsque l'installation est terminée, la fenêtre Fin de l'installation s'ouvre.

j. Cliquez sur Terminé.

   Le composant de collecte est installé.

3. Installez la console NFA :

   a. Double-cliquez sur le fichier RAConsoleSetup9.x.x.exe.

      La fenêtre de sélection de langue s'ouvre.

   b. Sélectionnez une langue, puis cliquez sur OK.

      La fenêtre de Bienvenue s'affiche.

   c. Cliquez sur Suivant.

      La fenêtre Contrat de licence s'affiche.

   d. Lisez et acceptez les termes du contrat de l'utilisateur final, puis cliquez sur Suivant.

      Votre système est testé pour vérifier qu'il répond à certaines conditions préalables. Si tel est le cas, le message Confirmation de regroupement s'affiche. Ce message identifie le chemin d'installation du composant de collecte, qui doit correspondre au chemin d'installation de la console NFA.

   e. Cliquez sur OK.

      La fenêtre Récapitulatif de la pré-installation s'ouvre.

   f. Cliquez sur Installer.

      Le processus d'installation démarre. Les messages indiquent la progression de l'installation. Lorsque l'installation est terminée, la fenêtre Fin de l'installation s'ouvre.

   g. Sélectionnez Yes, restart my system (Oui, redémarrer mon système).

h. Cliquez sur Terminé.

La console NFA est installée et votre système est prêt pour la configuration postérieure à l'installation (page 43).

Installations distribuées : si vous installez les composants CA Network Flow Analysis sur des serveurs distincts, reportez-vous directement aux rubriques suivantes :

- Installation du composant de collecte sur un serveur Windows (page 37)
- Installation du composant de collecte sur un serveur Linux (page 39)
- Installation de la console sur un serveur Windows (page 41)

Installation du composant de collecte sur un serveur Windows

Les configurations distribuées supposent des serveurs distincts pour la console NFA et pour le composant de collecte. Effectuez les opérations de cette rubrique pour installer le composant de collecte sur un serveur ou un ordinateur virtuel Windows dédié.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'utilisateur avec des droits d'administrateur.
2. Double-cliquez sur le fichier NFHarvesterSetup9.x.x.exe.

   La fenêtre de sélection de langue s'ouvre.
3. Sélectionnez une langue, puis cliquez sur OK.

   La fenêtre Contrat de licence s'affiche.
4. Lisez et acceptez les termes du contrat, puis cliquez sur Suivant.

   Votre système est testé pour vérifier qu'il répond à certaines conditions préalables. Si tel est le cas, la fenêtre Sélectionner le dossier d'installation s'ouvre.
5. (Facultatif) Lorsque vous y êtes invité, cliquez sur Sélectionner pour modifier l'emplacement d'installation ou entrez le chemin d'accès au nouvel emplacement.

   Remarque : Utilisez le même chemin d'installation pour les serveurs du composant de collecte et de la console NFA.

   L'emplacement par défaut est C:\CA\NFA. Il est recommandé d'installer les composants CA Network Flow Analysis sur le lecteur que vous avez configuré pour CA Network Flow Analysis, qui ne contient aucun système.

6. Cliquez sur Suivant.

   La boîte de dialogue Sélectionner l'emplacement du répertoire de données MySQL s'ouvre.

7. (Facultatif) Cliquez sur Sélectionner pour définir un emplacement distinct pour la base de données. Il est recommandé d'utiliser un lecteur comprenant 40 Go d'espace disponible minimum pour la base de données.

8. Cliquez sur Suivant.

   La boîte de dialogue Sélectionner l'emplacement temporaire du répertoire de données MySQL s'ouvre.

9. (Facultatif) Cliquez sur Sélectionner pour définir un emplacement distinct pour les fichiers temporaire de base de donnés ou entrez un nouvel emplacement manuellement. L'emplacement par défaut est C:\CA\NFA/MySql51/tmp.

10. Cliquez sur Suivant.

    La fenêtre Récapitulatif de la pré-installation s'ouvre.

11. Cliquez sur Installer.

    Le processus d'installation démarre. Les messages indiquent l'avancement de l'installation.

12. Lorsque l'installation est terminée, cliquez sur Finish (Terminer).

    Le composant de collecte est installé.

    Etape suivante : Installation de la console (page 41).

Installation du composant de collecte sur un serveur Linux

Les configurations distribuées supposent des serveurs distincts pour la console NFA et pour le composant de collecte. Effectuez les opérations détaillées dans cette rubrique pour installer le composant de collecte sur un serveur ou un ordinateur virtuel Linux dédié.

Remarque : Pour permettre la prise en charge des caractères non-latins, comme le chinois simplifié et le japonais, les clients de ligne de commande que vous utilisez pour l'installation doivent être configurés pour permettre le codage UTF-8. Si le codage UTF-8 n'est pas activé, ces caractères ne s'affichent pas correctement au cours de l'installation.

Les packs linguistiques appropriés sont également requis lors des déploiements de version localisée.

Procédez comme suit:

1. Connectez-vous à l'ordinateur cible en tant que qu'utilisateur root.

   Vous pouvez installer le logiciel localement ou à distance, par exemple, via ssh lorsque vous êtes connecté avec un compte root.

   Remarque : Si vous ne disposez pas d'un compte root, utilisez un compte disposant des droits sudo.

2. Ouvrez une invite de commande.

3. Exécutez la commande suivante pour modifier la limite des fichiers ouverts ulimit :
   ```
   ulimit -n valeur_ulimit
   ```

   Exemple :
   ```
   ulimit -n 65536
   ```

4. Exécutez la commande chmod sur le fichier d'installation pour qu'il soit exécutable :
   ```
   chmod u+x NFHarvesterSetup9.x.x.bin
   ```

5. Exécutez NFHarvesterSetup9.x.x.bin.

   La fenêtre de sélection de langue s'ouvre.

6. Sélectionnez une langue, puis cliquez sur OK.

   La boîte de dialogue Contrat de licence s’affiche.

7. Lisez et acceptez les termes du contrat, puis cliquez sur Suivant.

   La boîte de dialogue Sélectionner le répertoire d'installation s'ouvre.

8. (Facultatif) Cliquez sur Parcourir pour définir un emplacement d'installation. Vous pouvez installer le logiciel sur tous les systèmes de fichiers pour lequel l'utilisateur root dispose des droits d'accès en écriture. Le chemin par défaut est /opt/CA/NFA.
9. Cliquez sur Suivant.

   La boîte de dialogue Sélectionner l'emplacement du répertoire de données MySQL s'ouvre.
10. (Facultatif) Cliquez sur Sélectionner pour définir un emplacement distinct pour la base de données ou entrez un nouvel emplacement manuellement.

    Par défaut, la base de données MySQL est installée sous <répertoire_installation>/MySql51/data, où <répertoire_installation> est /opt/CA/NFA ou l'emplacement personnalisé spécifié à l'étape 8.

    Remarque : Vérifiez que l'emplacement sélectionné comprend 40 Go d'espace disponible minimum pour la base de données.
11. Cliquez sur Suivant.

    La boîte de dialogue Sélectionner l'emplacement temporaire du répertoire de données MySQL s'ouvre.
12. (Facultatif) Cliquez sur Sélectionner pour définir un emplacement distinct pour les fichiers temporaire de base de donnés ou entrez un emplacement personnalisé manuellement.

    Par défaut, l'emplacement est <répertoire_installation>/MySql51/tmp, où <répertoire_installation> est /opt/CA/NFA ou l'emplacement personnalisé spécifié à l'étape 8.
13. Cliquez sur Suivant.

    La fenêtre Récapitulatif de la pré-installation s'ouvre.
14. Cliquez sur Installer.

    Le processus d'installation démarre. La boîte de dialogue indique la progression de l'installation.

    Lorsque l'installation est terminée, vous êtes invité à quitter le programme d'installation.
15. Cliquez sur Terminer.

    Le composant de collecte est installé.

    Etape suivante : répétez ces étapes pour installer un composant de collecte sur un autre serveur ou reportez-vous à la rubrique suivante pour les étapes concernant l'installation de la console (page 41).

Installation de la console sur un serveur Windows

Les configurations distribuées utilisent des serveurs distincts pour la console NFA et pour le composant de collecte. Effectuez les opérations de cette rubrique pour installer la console NFA sur un serveur ou un ordinateur virtuel Windows dédié.

Procédez comme suit:

1. Connectez-vous au serveur en tant qu'utilisateur avec des droits d'administrateur.
2. Double-cliquez sur le fichier RAConsoleSetup9.x.x.exe.

   La fenêtre de sélection de langue s'ouvre.
3. Sélectionnez une langue, puis cliquez sur OK.

   La fenêtre de Bienvenue s'affiche.
4. Cliquez sur Suivant.

   La fenêtre Contrat de licence s'affiche.
5. Lisez et acceptez les termes du contrat de l'utilisateur final, puis cliquez sur Suivant.

   Votre système est testé pour vérifier qu'il répond à certaines conditions préalables. Si tel est le cas, la fenêtre Sélectionner le dossier d'installation s'ouvre.
6. (Facultatif) Lorsque vous y êtes invité, cliquez sur Sélectionner pour modifier l'emplacement d'installation du programme ou entrez le nouveau chemin d'accès manuellement.

   L'emplacement par défaut est C:\CA\NFA. Il est recommandé d'installer les composants CA Network Flow Analysis sur le lecteur que vous avez configuré pour CA Network Flow Analysis, qui ne contient aucun système. Utilisez le même chemin d'installation pour le composant de collecte et les serveurs de console.
7. Cliquez sur Suivant.

   La fenêtre Get Singlebox Configuration (Obtenir la configuration de regroupement) s'ouvre.
8. Sélectionnez Distributed (Distribuée), puis cliquez sur Suivant.

   La fenêtre Récapitulatif de la pré-installation s'ouvre.

9. Cliquez sur Installer.

   Le processus d'installation démarre. Les messages indiquent la progression de l'installation. Lorsque l'installation est terminée, la fenêtre Fin de l'installation s'ouvre.

10. Sélectionnez Yes, restart my system (Oui, redémarrer mon système).

11. Cliquez sur Terminé.

    La console est installée et votre système est prêt pour la configuration postérieure à l'installation (page 43).

Chapitre 5 : Tâches de post-installation

Ce chapitre traite des sujets suivants :

Procuration et installation de licences de produit (Windows) (page 43)
Synchronisation de l'heure système (Windows) (page 44)
Mise à jour de la liste des sites Internet approuvés (Windows) (page 44)
Modification des listes de contrôle d'accès au routeur (Windows) (page 45)

Procuration et installation de licences de produit (Windows)

Procurez-vous des licences CA Network Flow Analysis et NFM et enregistrez-les pour afficher les données CA Network Flow Analysis dans des rapports.

Procédez comme suit:

1. Procurez-vous les licences appropriées auprès du service clientèle de CA à partir du site de support en ligne de CA.
2. Enregistrez les fichiers de licence dans le répertoire <*chemin_installation*>\Licenses sur le serveur de la console NFA.
3. Effectuez l'une des tâches suivantes sur le serveur utilisé pour l'installation des fichiers de licence :
   - (Recommandé) Redémarrez le serveur.
   - Redémarrez les services CA Network Flow Analysis.
     a. Ouvrez la fenêtre Services.
     b. Cliquez avec le bouton droit de la souris sur le service MySql51 NetQoS et cliquez sur Redémarrer.
     Le message de confirmation de redémarrage des autres services s'ouvre et répertorie tous les services CA Network Flow Analysis dépendants.
     c. Cliquez sur Oui.
     Les services CA Network Flow Analysis redémarrent.

Synchronisation de l'heure système (Windows)

Synchronisez l'heure système de tous les serveurs sur lesquels les composants CA Network Flow Analysis sont installés. Effectuez les opérations suivantes sur chaque serveur, sauf si l'heure système est synchronisée automatiquement.

Procédez comme suit:

1. Cliquez avec le bouton droit de la souris sur la date ou l'heure dans la partie droite de la barre des tâches et sélectionnez Ajuster la date/l'heure.

   La boîte de dialogue Date et heure s'ouvre.

2. Cliquez sur l'onglet Temps Internet.
3. Cliquez sur Modifier les paramètres.

   La boîte de dialogue Paramètres d'heure Internet s'ouvre.

4. Cochez la case Synchroniser avec un serveur de temps Internet.
5. Sélectionnez le serveur pour la synchronisation. La valeur par défaut est time.windows.com.
6. Cliquez sur Mettre à jour.

   L'heure système est synchronisée avec le serveur sélectionné.

7. Dans la boîte de dialogue Paramètres d'heure Internet, cliquez sur OK.
8. Dans la boîte de dialogue Date et heure, cliquez sur OK.

Remarque : Si certaines unités de collecte se trouvent dans différents fuseaux horaires, définissez chaque unité en fonction du fuseau horaire local. Les heures sont converties en heures de Greenwich (GMT).

Mise à jour de la liste des sites Internet approuvés (Windows)

Ajoutez le serveur de console à la liste des sites Internet approuvés. Le processus varie selon le navigateur. Les instructions suivantes correspondent à Microsoft Internet Explorer.

Procédez comme suit :

1. Lancez Internet Explorer sur l'ordinateur de console.
2. Cliquez sur Outils, Options.
3. Dans l'onglet Sécurité, cliquez sur l'icône Sites de confiance.

4. Cliquez sur Sites.
5. Dans le champ Ajouter ce site Web à la zone, entrez **http://hôte_local**.
6. Cliquez sur Ajouter.

Modification des listes de contrôle d'accès au routeur (Windows)

Si la console NFA et des composants de collecte sont installés sur des serveurs distincts, les listes de contrôle d'accès au routeur doivent être configurées pour permettre aux composants de collecte d'effectuer des interrogations SNMP.

Remarque : Si les interfaces de bouclage utilisent les paquets de flux en tant que sources, vérifiez que CA Network Flow Analysis peut accéder aux adresses IP de ces interfaces.

Index

.

.NET
  version de .NET Framework requise - 10

A

affichage
  résolution d'affichage requise - 10
anti-espiogiciels
  désactivation sur les serveurs d'installation - 33
ASP
  configuration (Windows) - 15

C

CA Performance Center
  version requise - 33
COM+
  configuration (Windows) - 15
Composant de collecte
  configuration requise pour les serveurs (Linux) - 27
  configuration requise pour les serveurs (Windows) - 12
  installation sur un serveur autonome (Windows) - 35
  installation sur un serveur dédié (Windows) - 37
compression d'espace disque
  raisons pour l'éviter - 33
conditions requises
  conditions d'installation requises - 33
configuration distribuée
  configuration matérielle requise - 12
  installation de la console sur un serveur dédié (Windows) - 41
  installation du composant de collecte sur un serveur dédié (Linux) - 39
  installation du composant de collecte sur un serveur dédié (Windows) - 37
Console NFA
  configuration requise pour les serveurs (Windows) - 12
  installation sur un serveur autonome (Windows) - 35
  installation sur un serveur dédié (Windows) - 41
contenu Web
  configuration pour une expiration immédiate - 19
Corbeille
  suppression immédiate des fichiers - 24
courriel
  configuration des restrictions de relais SMTP - 22

E

environnement d'exécution (JRE)
  version de l'environnement d'exécution Java requise - 10

F

Firefox
  versions prises en charge (Linux) - 27
  versions prises en charge (Windows) - 11
Flash Player
  t - 15

G

Gestionnaire de serveur, fenêtre
  configuration des services IIS, COM+ et ASP - 15
  configuration des services SNMP et SMTP - 18
  configuration du nom de communauté public - 20

I

IIS
  configuration (Windows) - 15
  configuration de l'expiration du contenu Web - 19

configuration des restrictions de relais SMTP - 22
Internet Explorer
désactivation temporaire du mode de compatibilité - 11
versions prises en charge (Windows) - 11
iptables (Linux)
désactivation pour l'ouverture de ports - 30

L

langues
options prises en charge - 10, 27
licences
demande, installation - 43
Linux
version/navigateur pris en charge - 27

M

mode de compatibilité pour Internet Explorer
désactivation temporaire - 11

N

navigateurs
pris en charge pour Linux - 27
pris en charge pour Windows - 11
nom de communauté
configuration du nom public - 20
nom de communauté public
configuration (Windows) - 20

O

outils de surveillance/de maintenance de serveur
désactivation sur les serveurs d'installation - 33

P

Pare-feu
désactivation d'iptables (Linux) - 30
ports à ouvrir (Windows) - 14
ports
ports à ouvrir dans le pare-feu (Windows) - 14

R

Reader
configuration requise pour Adobe Reader - 15
répertoire tmp (Linux)
déplacement - 27

S

service SNMP
configuration à partir de la fenêtre Gestionnaire de serveur - 18
modification des listes de contrôle d'accès du routeur - 45
services
désactivation des services non requis - 25
services de rôle
configuration (Windows) - 15
SMTP
configuration à partir de la fenêtre Gestionnaire de serveur - 18
configuration des restrictions de relais SMTP - 22
stratégie DEP
activation (Windows) - 23
système autonome
configuration matérielle requise pour les serveurs (Windows) - 13
procédure d'installation (Windows) - 35
systèmes d'exploitation
systèmes d'exploitation Windows pris en charge - 10

T

t
configuration requise pour les serveurs Linux - 27
configuration requise pour les serveurs Windows - 10
temps système
synchronisation - 44
time
synchronisation du temps système - 44

W

Windows
    version prise en charge - 10